	COUNTY OF SAN BERNARDINO POLICY	No. 2-362 Issue No. 1 Effective: January 3, 2006 Page 1 of 3 By: Bea Valdez, Interim Chief of Administrative Services
	PUBLIC HEALTH	Approved: James A. Felten Public Health Director
Subject: SYSTEMS USE AND SECURITY		

I. POLICY:

It is the policy of the Department of Public Health (DPH) to provide systems to facilitate DPH workforce members' job functions and help in fulfilling job requirements. Each workforce member has the responsibility to use dedicated systems professionally, ethically, lawfully and in compliance with all applicable policies.

II. PURPOSE:

The purpose of this policy is to provide DPH workforce members with direction regarding the appropriate use of systems.

III. SYSTEMS USE:

A system consists of computers, desktops, laptops, software applications, servers and networks or network services.

A. Workforce members must:

1. Only use systems that have been approved and installed by Information Technology (IT).
2. Comply with all applicable policies listed in the reference section below.

B. Workforce members shall not:

1. Send departmental proprietary or confidential information to anyone not entitled to know or possess such information.
2. Intentionally disrupt a network service.
3. Deliberately perform acts that waste system resources or unfairly monopolize resources to the exclusion of others.
4. Download or store audio, video, picture files unless these files are required to perform operational responsibilities.
5. Load any unauthorized software.
6. Remove any authorized software placed by IT.
7. Copy DPH software for use on their home computers (unless authorized).
8. Modify, revise, transform, recast or adapt any software or reverse-engineer, disassemble or decompile any software.
9. Install custom screen savers without approval from IT.
10. Post or send threatening or offensive messages.

IV. SYSTEMS SECURITY:

Information Technology is responsible for ensuring that all systems used to access, transmit, receive or store information are appropriately secured in accordance with this policy. To ensure security:

1. Servers must be located in a physically secure environment, and on a secure network with firewall protection.
2. Intrusion Detection Systems (IDS) should be used to warn of unusual or undesirable traffic on the network.
3. Encryption of data in transport or at rest should be implemented when required or at the discretion of Information Technology.
4. A user identification and password authentication mechanism must be implemented to control user access to systems.
5. All relevant security patches and updates must be promptly applied to mitigate any known vulnerabilities.
6. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
7. An automatic logoff or inactivity timeout mechanism must be implemented
8. All unused or unnecessary services shall be disabled.
9. The use of a screen guard or privacy screen is recommended where unauthorized viewing concerns requires additional security measures. Program Managers or their designees should evaluate system areas to ensure that system screens or displays are situated in a manner that prohibits unauthorized viewing.

V. SYSTEMS MONITORING:

Workforce members using DPH systems should have no expectation of privacy. DPH, at its discretion may log, review, or monitor any data stored or transmitted on its information systems to manage those assets to ensure compliance with applicable policies.

VI. VIOLATIONS:

Failure to comply with this policy may result in disciplinary action up to and including termination of employment/contract.

VII. REFERENCE:

A. Related County Policies

1. 14-01, Electronic Mail (E-Mail) Systems
2. 14-04, Internet/Intranet Use Policy

B. Related DPH Policies

1. 2-312, Administrative, Physical and Technical Safeguards
2. 2-350, Information Security
3. 2-364, Access Control
4. 2-366, Transmission Security

C. References

- Health Insurance Portability and Accountability Act Code of Federal Regulations (CFR) Parts 160 and 164